# AI Resilience Maturity Model (AI-RMM)

### AI-Related Risk Management Process Guide ISO 31000

### Introduction

This guide presents a structured framework for managing AI-related risks within organizations, grounded in the principles of the ISO 31000 risk management standard. It aims to assist organizations in embedding risk management into their AI initiatives, ensuring that AI technologies are deployed and used responsibly, securely, and effectively. Adhering to ISO risk management processes ensures a universally recognized approach, enhancing the organization's ability to manage AI risks systematically.

### 1. Establishing the Context

### 1.1 Define the Scope

Clearly define the scope of AI applications within your organization, understanding the objectives, stakeholders, and the decision-making environment of each AI system.

### 1.2 Identify Internal and External Context

Assess both the internal context (organizational culture, structure, resources) and the external context (regulatory landscape, technological advancements, societal expectations) that influence AI risk management.

### 2. Risk Identification

### 2.1 AI System Inventory

Catalog all AI systems in use, detailing their purposes, inputs, outputs, and the environments in which they operate.

### 2.2 Identify AI Risks

Pinpoint potential risks associated with AI systems, considering factors like data integrity, algorithmic bias, ethical implications, and operational dependencies.

### 3. Risk Analysis

### 3.1 Analyze Risk Characteristics

Examine the nature of identified risks, including their causes, sources, and potential impact on organizational objectives and stakeholder well-being.

### 3.2 Determine Risk Level

Assess the likelihood and impact of each risk to determine its level. This involves both qualitative judgments and quantitative analyses where feasible.

### 4. Risk Evaluation

### 4.1 Prioritize Risks

Evaluate the risks in the context of your organizational risk criteria to prioritize them. This helps focus attention and resources on managing the most significant risks.

### 4.2 Decision Making

Decide on the most appropriate risk treatment options for high-priority risks, considering the organization's risk appetite and capacity for risk management.

### 5. Risk Treatment

### 5.1 Develop Risk Treatment Plans

Formulate specific strategies for mitigating, transferring, avoiding, or accepting each significant risk, outlining actionable steps, responsibilities, and timelines.

### 5.2 Implement Risk Treatments

Execute the treatment plans, applying the necessary controls and measures to manage the prioritized risks effectively.

### 6. Monitoring and Review

### 6.1 Continuous Monitoring

Establish ongoing monitoring processes to track the performance of risk treatments, the emergence of new risks, and changes in the external and internal context.

### 6.2 Regular Reviews

Periodically review the risk management process and its outcomes to ensure its effectiveness and relevance. Adjust risk assessments, treatments, and strategies based on these reviews.

### 7. Communication and Consultation

### 7.1 Stakeholder Engagement

Engage with stakeholders throughout the risk management process, ensuring clear communication and understanding of risk-related information, decisions, and actions.

### 7.2 Transparency

Maintain transparency in risk management practices, decisions, and outcomes to build trust and ensure informed participation by all relevant parties.

### Conclusion

Adhering to ISO risk management processes for AI-related risks enables organizations to navigate the complexities of AI deployment with confidence. This structured approach ensures that risks are managed proactively, decisions are informed, and AI technologies contribute positively to organizational goals and societal well-being.